REMARKS

Claims 1-8, 10-17, 21-25, and 36-38 are pending. Claims 1-7, 10-17, 21-25, and 36-38 are rejected under 35 U.S.C. 102(e) by *Touboul* (U.S. Pat. No. 6,804,780 B1). Claim 8 is rejected under 35 U.S.C. 103(a) by *Touboul* further in view of *Smithson* et al. (U.S. Pat. No. 6,898,715).

With respect to claim 1, the Office action cites the *Touboul* reference as describing a "URL comparator" that examines a URL of a "Downloadable" against the URLs in a rule database. It does so using a security policy. The results are sent to a "log engine" where a "policy selector" is used to determine whether the Downloadable is harmful or not. This is not the same as components recited in claim 1 including a scan module or the act of scanning a protocol field and identifying a content-related protocol.

Also with respect to claim 1, the Office action cites portions of *Touboul* that describe a security policy editor that allows users to modify security policies. One example cited is editing URLs in the URL rule database. This disclosure from *Touboul* does not teach or show a proxy module adding a re-direction header to a request so that it goes to a proxy server as recited in claim 1. Nor does it anticipate a proxy server's content scanning module and user-defined configuration data scanning module as recited in claim 1.

With respect to independent claim16, the Office action cites from *Touboul* a "first comparator" that determines whether a Downloadable should be tested, as provided for in a security policy. A certificate scanner scans the Downloadable for a certificate and a "certificate comparator" compares the scanned certificate with certificates on a trusted list. This is not the same as decoding a response or scanning the decoded response as recited in claim 16. The Office action also cites a flow chart description in *Touboul* for determining whether to block a Downloadable. In the description of this flow diagram, there is no disclosure or mention of processing a request using user-defined configuration data as recited in the claimed invention.

The Office Action also cites the *Smithson* reference with respect to claim 8. Smithson does not teach a proxy server quarantining undesirable content as recited in the claim. Smithson teaches various counter measures, but none include the act of quarantining. One counter

measure is automatically sending a copy of detected viruses to a remote site for analysis. However, this does not anticipate the step of quarantining undesirable content in a network.

Applicant believes that all pending claims are allowable and respectfully requests a Notice of Allowance for this application from the Examiner.

Respectfully submitted,

/Rupak Nag/

Rupak Nag
Reg. No. 37,493

Beyer Weaver LLP
P.O. Box 70250
Oakland, CA 94612-0250
Telephone: (612) 252-3335